Sistem Keamanan Pintu Menggunakan Sensor Sidik Jari Berbasis Node MCU V3

Hidayat Efendi [a,1,*], Muhammad Ihsan[b,2], Dedi Haryanto [c,3]

[a, b, c] Teknologi Informasi, Fakultas Teknik, Universitas Muhammadiyah Palembang, Indonesia
[1]hidayatefendi2004@gmail.com*; [2]Ihsan_idris@um-palembang.ac.id, [3]dediharyanto@gmail.com
* Penulis Korespondensi

ABSTRAK

Keamanan pintu merupakan salah satu aspek penting dalam melindungi aset dan membatasi akses terhadap suatu ruangan. Penggunaan kunci konvensional masih memiliki kelemahan, seperti risiko kehilangan, kerusakan, atau duplikasi kunci oleh pihak yang tidak berwenang. Penelitian ini bertujuan untuk merancang dan membangun sistem keamanan pintu menggunakan sensor sidik jari berbasis NodeMCU V3 yang terintegrasi dengan teknologi Internet of Things (IoT). Sistem ini memanfaatkan sensor fingerprint sebagai media autentikasi pengguna, solenoid sebagai pengunci pintu elektronik, serta aplikasi Telegram sebagai media monitoring dan notifikasi jarak jauh. Metode penelitian yang digunakan meliputi analisis kebutuhan, perancangan sistem, implementasi perangkat keras dan perangkat lunak, serta pengujian sistem. Hasil pengujian menunjukkan bahwa sistem mampu mengenali sidik jari yang terdaftar dengan baik, mengontrol pembukaan pintu secara otomatis, serta mengirimkan notifikasi kepada pengguna. Sistem yang dikembangkan dapat meningkatkan keamanan dan memberikan kemudahan dalam pengelolaan akses pintu secara lebih efektif dan modern.

Riwayat Artikel
Diterima 11 Febuari 2026
Diperbaiki 21 Februari 2026
Diterbitkan 28 Febuari 2026

Kata Kunci
Sistem keamanan pintu
Fingerprint
NodeMCU V3
Internet of Things
Telegram

1. Pendahuluan

Teknologi akses ke dalam sebuah ruangan pun mengalami perkembangan yang sebelumnya menggunakan kunci manual berubah menjadi dengan password atau sidik jari[1].[2]. Akses pada suatu ruangan yang sangat rahasia atau ruangan khusus dan tidak sembarang orang bisa akses pada ruangan tersebut seharusnya sudah menggunakan metode akses kontrol, sehingga hanya orang-orang tertentu saja yang mempunyai hak akses ruangan tersebut[3]. Dengan menggunakan metode ini akan mengatasi sering terjadinya kehilangan kunci dan kesulitan untuk menentukan kunci yang akan digunakan untuk membuka suatu ruangan, dikarenakan semakin banyak ruangan maka akan semakin banyak pula kunci yang harus disediakan sehingga dibutuhkan waktu untuk pencarian kunci yang tepat[4].

Kasus pencurian yang sering terjadi di gudang, rumah, dan toko dapat menimbulkan ancaman kerugian serta keamanan bagi pemiliknya. Oleh karena itu, perlu adanya sistem keamanan yang baik untuk melindungi aset tersebut. Salah satu komponen penting dalam sistem keamanan adalah pintu, yang merupakan akses utama masuk ke dalam suatu ruangan[5]. Dengan demikian, penggunaan sistem keamanan yang efektif pada pintu sangat dibutuhkan. Namun, salah satu tantangan dalam implementasi alat-alat IoT adalah masalah jaringan internet[6]. Untuk menjawab hal ini, pilihan provider atau penyedia jaringan internet harus dipertimbangkan dengan hati-hati agar tidak mengalami gangguan.

Kunci konvensional memiliki kelemahan, terutama terkait risiko pencurian atau duplikasi, yang dapat memungkinkan pihak yang tidak berhak masuk ke dalam rumah[7]. Mayoritas masyarakat masih mengandalkan kunci konvensional untuk mengamankan rumah mereka, meskipun terdapat kekhawatiran terhadap potensi kehilangan kunci yang membuka peluang akses tidak sah. Selain itu, proses penggantian kunci setelah kehilangan sering kali memakan waktu dan biaya, sehingga

Jurnal Sarjana Teknik Informatika
Vol. 14., No. 1, Februari 2026, pp. 63-69

menambah beban bagi penghuni perumahan. Oleh karena itu, solusi inovatif dalam sistem keamanan pintu menjadi semakin penting untuk meningkatkan keamanan dan kenyamanan[8]. Salah satu solusi yang dapat diterapkan adalah pengembangan sistem keamanan pintu berbasis sensor sidik jari yang terintegrasi dengan teknologi *Internet of Things* (IoT) menggunakan NodeMCU V3 sebagai pengendali utama[9].

kebaruan (*novelty*) dalam penelitian ini terletak pada integrasi autentikasi biometrik sidik jari dengan sistem notifikasi dan pemantauan real-time berbasis IoT melalui *platform* komunikasi digital, sehingga pengguna tidak hanya memperoleh sistem penguncian elektronik tetapi juga sistem monitoring jarak jauh[10]. Selain itu, penelitian ini mengembangkan mekanisme pencatatan log akses pengguna yang tersimpan secara digital, sehingga riwayat keluar-masuk ruangan dapat terdokumentasi dengan lebih sistematis dibandingkan sistem kunci konvensional maupun sistem elektronik sederhana yang belum terintegrasi jaringan[11]**.**

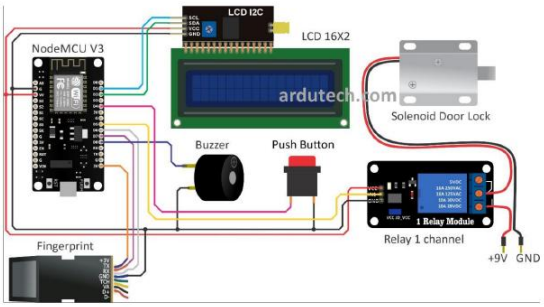
Berdasarkan uraian tersebut, penelitian ini mengembangkan sistem keamanan pintu dengan judul "Sistem Keamanan Pintu Menggunakan Sensor Sidik Jari Berbasis NodeMCU V3" sebagai solusi untuk meningkatkan efektivitas pengendalian akses dan pemantauan keamanan ruangan.

2. Metode

Penelitian ini menggunakan model pengembangan Prototype. Metode ini dipilih karena sistem yang dikembangkan berbasis integrasi perangkat keras dan perangkat lunak (IoT), sehingga memerlukan proses perancangan dan pengujian berulang hingga diperoleh sistem yang stabil dan sesuai kebutuhan [12].

2.1. Perancangan sistem

Perangkat keras sistem terdiri dari NodeMCU V3 (ESP8266), sensor sidik jari tipe AS608, modul relay, solenoid door lock, dan catu daya [13]. Arsitektur sistem dirancang dengan konsep input process output, di mana sensor sidik jari sebagai input, NodeMCU sebagai unit pemroses, dan relay serta solenoid sebagai perangkat keluaran untuk membuka pintu. Komunikasi antara sensor dan NodeMCU menggunakan protokol serial UART.



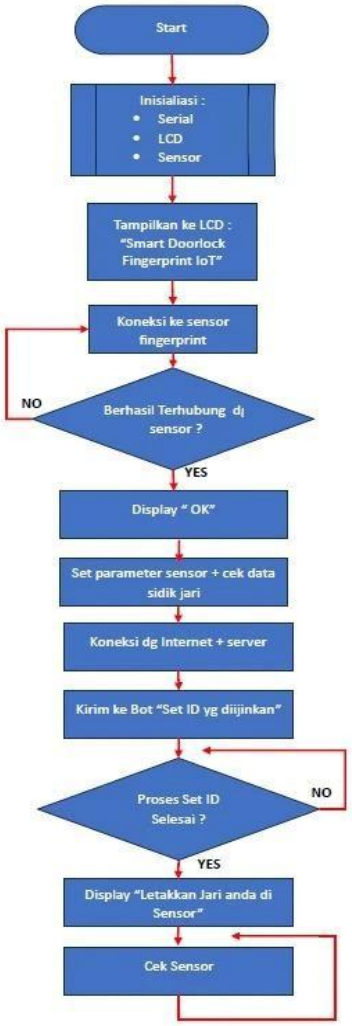
.

Gambar 1 Perancangan sistem

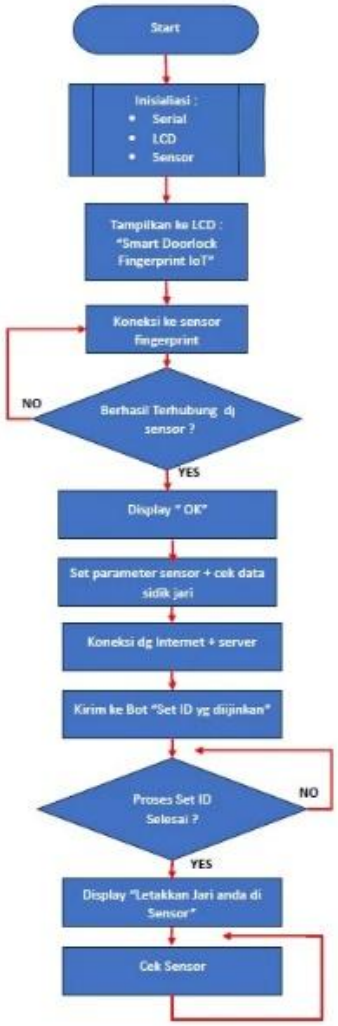
Gambar 2 pada tahap awal, sistem melakukan inisialisasi komunikasi serial, LCD, serta sensor fingerprint untuk memastikan seluruh komponen siap digunakan. Setelah proses inisialisasi selesai, LCD menampilkan pesan awal seperti instruksi pendaftaran atau pemindaian sidik jari. Sistem kemudian melakukan pengecekan koneksi sensor *fingerprin*t. Jika sensor belum terhubung dengan baik, sistem akan terus melakukan pengecekan hingga koneksi berhasil. Apabila sensor terdeteksi dan terhubung, status "OK" ditampilkan sebagai indikator bahwa perangkat siap beroperasi.

Gambar 3 Setelah sensor dinyatakan aktif, sistem mengatur parameter sidik jari dan mempersiapkan data pengguna. Pada tahap ini, NodeMCU melakukan koneksi ke jaringan internet dan server yang digunakan untuk integrasi IoT[14]. Jika koneksi berhasil, sistem mengirimkan notifikasi melalui bot Telegram sebagai bentuk monitoring jarak jauh. Proses pendaftaran atau pengaturan ID sidik jari dilakukan hingga data tersimpan dengan benar. Apabila proses belum

selesai, sistem akan mengulangi tahapan pengaturan hingga berhasil, kemudian perangkat kembali ke kondisi siaga.



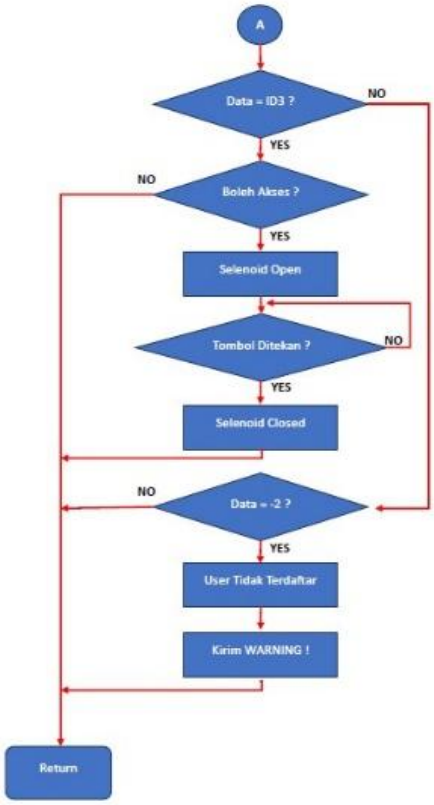
Gambar 2 flowchart kerja alat



Gambar 3 Flowchart verifikasi sidik jari

Gambar 4 autentikasi dan pengendalian akses pintu. Ketika pengguna menempelkan jari pada sensor, sistem membaca ID sidik jari dan membandingkannya dengan database yang telah tersimpan. Jika ID terdaftar dan memiliki izin akses, maka sistem mengaktifkan mekanisme pembuka pintu dan menampilkan status pintu dalam kondisi terbuka. Setelah jangka waktu tertentu atau setelah tombol ditekan, pintu akan kembali tertutup secara otomatis. Sebaliknya, jika ID tidak terdaftar atau tidak memiliki hak akses, sistem tidak akan membuka pintu dan akan mengirimkan notifikasi peringatan melalui Telegram sebagai indikasi adanya upaya akses yang tidak sah. Setelah proses tersebut selesai, sistem kembali ke kondisi awal dan siap menerima input berikutnya.

Jurnal Sarjana Teknik Informatika
Vol. 14., No. 1, Februari 2026, pp. 63-69



Gambar 4 Flowchart sidik

Secara keseluruhan, ketiga flowchart tersebut menggambarkan alur sistem yang dimulai dari inisialisasi perangkat, konfigurasi dan integrasi IoT, hingga proses autentikasi pengguna serta pengendalian akses pintu secara *real-time* dan terdokumentasi secara digital [15].

3. Hasil dan Pembahasan

Pengujian dilakukan untuk mengetahui kinerja sistem keamanan pintu berbasis sensor sidik jari dan NodeMCU V3, khususnya pada aspek akurasi identifikasi, kecepatan respons, dan performa notifikasi berbasis jaringan. Pengujian melibatkan 20 pengguna yang telah didaftarkan ke dalam sistem.

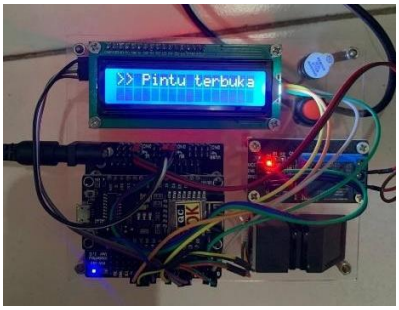
3.1. Gambaran Uji Coba Sistem

Uji coba dilakukan untuk mengevaluasi kinerja sistem keamanan pintu berbasis sensor sidik jari dan NodeMCU V3 pada aspek akurasi, waktu respons, dan delay notifikasi IoT. Sebanyak 20 pengguna didaftarkan ke dalam sistem, kemudian dilakukan 200 kali percobaan autentikasi untuk mengukur tingkat keberhasilan identifikasi. Pada setiap pengujian, sidik jari yang dipindai dibandingkan dengan data yang tersimpan. Jika sesuai, NodeMCU V3 mengaktifkan solenoid door lock untuk membuka pintu, dan waktu dihitung sejak pemindaian dimulai hingga pintu terbuka. Pengujian waktu respons dilakukan sebanyak 50 kali untuk memperoleh nilai rata-rata.

Sistem juga diuji dalam kondisi terhubung ke jaringan WiFi untuk mengukur delay pengiriman notifikasi. Delay dihitung sejak autentikasi berhasil hingga notifikasi diterima pada perangkat pengguna. Secara umum, sistem berjalan stabil selama pengujian. Variasi hasil lebih dipengaruhi oleh posisi jari dan kondisi jaringan dibandingkan oleh kinerja perangkat keras.

Gambar 5 Tampilan sidik jari yang terdaftar dan diberi akses izin masuk

Gambar 5 menampilkan hasil pengujian sistem saat sidik jari yang telah terdaftar ditempelkan pada sensor fingerprint. Sistem berhasil mengenali identitas pengguna dan memverifikasi bahwa sidik jari memiliki izin akses. Informasi status akses ditampilkan pada LCD sebagai tanda bahwa proses autentikasi berhasil dilakukan.



Gambar 6 Tampilan Pintu Terbuka (Selenoid Terbuka)

Gambar 6 menunjukkan kondisi pintu dalam keadaan terbuka setelah proses verifikasi sidik jari berhasil. NodeMCU mengaktifkan solenoid sebagai mekanisme pengunci elektronik sehingga pintu dapat terbuka secara otomatis. Setelah proses selesai, sistem kembali ke kondisi standby untuk menunggu input berikutnya.

3.2. Hasil Pengujian

Pengujian sistem dilakukan untuk mengetahui kinerja secara kuantitatif. Parameter yang diuji meliputi tingkat akurasi autentikasi, waktu respons pembukaan pintu, serta delay notifikasi berbasis jaringan. Berdasarkan hasil pengujian, sistem menunjukkan performa yang stabil dengan tingkat akurasi sebesar 97,0%, rata-rata waktu respons 1,38 detik, dan rata-rata delay notifikasi 412 milidetik. Hasil ini menjadi dasar analisis lebih lanjut terhadap keandalan dan efisiensi sistem yang dikembangkan.

Tabel 1 Hasil Pengujian Akurasi Sistem Autentikasi Sidik Jari

No	Parameter Pengujian	Jumlah	Persentase (%)
1.	Total percobaan autentifikasi	200	100%
2.	Autentifikasi berhasil	194	97,0 %
3.	Autentikasi gagal	6	3,0 %

e-ISSN: 2809-3399, p-ISSN: 2338-5197 Vol. 14., No. 1, Februari 2026, pp. 63-69

Pengujian dilakukan terhadap 20 pengguna yang telah terdaftar pada sistem. Setiap pengguna melakukan beberapa kali percobaan pemindaian hingga total mencapai 200 pengujian. Kegagalan autentikasi terjadi akibat faktor posisi jari yang tidak stabil dan kondisi permukaan sensor. Tingkat akurasi dihitung berdasarkan perbandingan antara jumlah autentikasi berhasil dengan total percobaan.

Tabel 2 Hasil Pengujian Waktu Respons Sistem

No	Parameter Pengujian	Nilai (detik)
1.	Jumlah pengujian	50 kali
2.	Waktu respons tercepat	1,12
3.	Waktu respons terlama	1,74
4.	Rata-rata waktu respons	1,38

Waktu respons dihitung sejak sensor sidik jari mulai membaca data hingga solenoid door lock aktif membuka pintu. Pengujian dilakukan sebanyak 50 kali dalam kondisi sistem berjalan normal tanpa gangguan jaringan. Nilai rata-rata diperoleh dari keseluruhan waktu respons yang tercatat selama pengujian.

Tabel 3 Hasil Pengujian Delay Notifikasi

No	Parameter Pengujian	Nilai (ms)
1.	Jumlah Pengujian	50 kali
2.	Delay Tercepat	320
3.	Delay Terlama	587
4.	Rata rata delay notifikasi	412

Delay dihitung sejak data autentikasi berhasil diproses oleh NodeMCU V3 hingga notifikasi diterima pada perangkat pengguna melalui jaringan WiFi. Pengujian dilakukan pada kondisi jaringan stabil dengan kecepatan rata-rata 20 Mbps. Variasi delay dipengaruhi oleh latensi jaringan dan trafik data saat pengujian berlangsung.

4. Kesimpulan

Berdasarkan keseluruhan hasil pengujian, sistem keamanan pintu berbasis sensor sidik jari dan NodeMCU V3 menunjukkan performa yang stabil dan konsisten. Tingkat akurasi sebesar 97,0% membuktikan bahwa proses autentikasi mampu meminimalkan kesalahan identifikasi. Waktu respons rata-rata 1,38 detik memperlihatkan bahwa sistem bekerja secara cepat dan tidak menimbulkan jeda yang signifikan bagi pengguna. Sementara itu, rata-rata delay notifikasi sebesar 412 milidetik masih berada dalam batas toleransi sistem berbasis Internet of Things.

Jika dianalisis secara menyeluruh, performa sistem lebih dipengaruhi oleh faktor eksternal seperti posisi jari dan kondisi jaringan dibandingkan oleh keterbatasan perangkat keras. NodeMCU V3 mampu menjalankan proses autentikasi dan pengendalian aktuator secara efisien tanpa mengalami penurunan kinerja selama pengujian berlangsung.

Hasil ini menunjukkan bahwa rancangan sistem tidak hanya berfungsi secara konseptual, tetapi juga memenuhi parameter kinerja yang dibutuhkan untuk implementasi nyata. Dengan kombinasi akurasi tinggi, waktu respons cepat, dan kemampuan integrasi jaringan, sistem yang dikembangkan layak digunakan sebagai solusi keamanan ruangan berbasis biometrik.

Deklarasi

Kontribusi Penulis. Seluruh penulis berkontribusi secara aktif dalam penelitian ini, mulai dari perancangan sistem, implementasi perangkat keras dan perangkat lunak, proses pengujian, analisis data, hingga penyusunan dan penyempurnaan naskah artikel. Semua penulis telah membaca, meninjau, dan menyetujui versi akhir artikel yang diajukan untuk dipublikasikan.

Pernyataan pendanaan. Penelitian ini tidak menerima pendanaan khusus dari lembaga pemerintah, swasta, maupun institusi lainnya.

Konflik kepentingan. Penulis menyatakan tidak terdapat konflik kepentingan dalam pelaksanaan penelitian maupun penyusunan artikel ini.

Informasi tambahan. Tidak terdapat informasi tambahan yang berkaitan dengan artikel ini.

Daftar Pustaka

[1] C. N. Insani and N. Arifin, "IoT-Enabled Real-Time Monitoring and Tsukamoto Fuzzy Classification of Mandar River Water Quality via Web Integration for Sustainable Resource Management," *Jurnal Teknik Informatika (Jutif)*, vol. 6, no. 5, pp. 3079–3092, 2025, doi: 10.52436/1.jutif.2025.6.5.5249.

[2] T. Nguyen and H. Tran, "Performance evaluation of ESP8266 for IoT applications," *Journal of Engineering and Technology*, vol. 18, no. 4, pp. 211–220, 2022.

[3] J. Y. Kim, C. H. Chu, and S. M. Shin, "ISSAQ: An Integrated Sensing System for Real-Time Indoor Air Quality Monitoring," *IEEE Sens. J.*, vol. 14, no. 12, pp. 4230–4244, 2014, doi: 10.1109/JSEN.2014.2359832.

[4] M. Flores-Iwasaki, G. A. Guadalupe, and M. Pachas-Caycho, "Internet of Things (IoT) Sensors for Water Quality Monitoring in Aquaculture Systems: A Systematic Review and Bibliometric Analysis," *AgriEngineering*, vol. 7, no. 3, p. 78, 2025, doi: 10.3390/agriengineering7030078.

[5] L. Atzori, A. Iera, and G. Morabito, "Understanding the Internet of Things: Definition and challenges," *Computer Networks*, vol. 200, pp. 108–121, 2022.

[6] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, 2021.

[7] P. Gope and T. Hwang, "BSN-Care: A secure IoT-based healthcare system," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1576–1587, 2021.

[8] J. Smith and L. Brown, "Design and implementation of fingerprint-based smart lock system," *Int. J. Embed. Syst.*, vol. 14, no. 2, pp. 101–110, 2023.

[9] K. Ashton, "That Internet of Things thing," *RFID Journal*, vol. 22, no. 7, pp. 97–114, 2021.

[10] D. Evans, "The Internet of Things: How the next evolution of the Internet is changing everything," Cisco White Paper, 2021.

[11] M. A. Al-Garadi, "A survey of machine and deep learning methods for IoT security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2021.

[12] A. Kumar and D. Zhang, "Personal recognition using hand shape and texture," *IEEE Transactions on Image Processing*, vol. 15, no. 8, pp. 2454–2461, 2021.

[13] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Secur. Priv.*, vol. 19, no. 2, pp. 33–42, 2022.

[14] A. Rahman, S. Islam, and M. Hasan, "Secure access control system using biometric authentication," *IEEE Access*, vol. 11, pp. 33456–33468, 2023.

[15] T. Malinda, I. Salamah, and N. Anugraha, "Implementation of an IoT-based Threshold Method for a Food Hazardous Substance Detection Tool," *SISFOKOM (Sistem Informasi dan Komputer)*, vol. 14, no. 3, pp. 401–406, 2025, doi: 10.32736/sisfokom.v14i3.2397.